March 22, 2021

Via email: comments@fdic.gov; regs.comments@federalreserve.gov.

Chief Counsel's Office
Attention: Comment Processing,
Office of the Comptroller of the Currency,
400 7th Street SW, Suite 3E–218, Washington, DC 20219

Ann E. Misback,
Secretary, Board of Governors of the Federal Reserve System,
20th Street and Constitution Avenue NW, Washington, DC 20551

Hames P. Sheesley,
Assistant Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation,
550 17th Street NW, Washington, DC 20429

Re: Proposed rule titled: Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers. Docket ID OCC–2020–0038; Docket No. R–1736, published at 86 Fed. Reg. 2299 (Jan.12, 2021).

I respectfully submit the following comments to the Office of the Comptroller of the Currency, the Federal Reserve System, and the Federal Deposit Insurance Corporation regarding the proposed rule titled "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers." The proposed rule would be codified at 12 CFR Part 53, 225, and 304.

These comments are submitted by Atticus Yondorf, a law student interested in administrative law and banking regulations. I submit these comments in my individual capacity and not on behalf of any organization.

I. I write in support the proposed rule. First, notifications under the current regulatory scheme are inadequate. The potential threats posed by contemporary hackers and system failures—such as those caused by natural catastrophes–either go unmonitored or are brought to the attention of appropriate agencies too late. The proposed rule addresses the current lack of targeted notification by creating a separate notification process, an important step toward properly addressing the current threats.

Second, the notification requirements are unlikely to be overly burdensome for banking institutions. The cost of compliance would be less onerous than those currently incurred for Suspicious activity reports (SRAs). Furthermore, this cost is relatively small in comparison to the benefits of increased capacity for appropriate agencies to view defects in the banking system which would inevitably be identified through the rule's targeted notification process.

Third, the notification requirements would, after a sufficient time, provide a substantial amount of data to agencies from which they will be able to pinpoint where and how the current banking system is vulnerable to cyber hacks, among other covered acts. The notification requirement in other words, could provide a strong impetus for more regulation where if and when it is needed.

I do have two concerns about the proposed rule, however.

II. My first concern is also a response to the first and tenth question posed in the notice. Either the definition of what constitutes an incident is too narrow, or the definition of bank service provider, or more broadly the regulated parties, is too narrow, if this rule is to effect the result it intends.

Currently, the proposed rule defines a computer-security incident as an occurrence that (i) results in actual or potential harm to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits; or (ii) constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. This definition does not appear to include hacks/significant catastrophic events that infiltrate/impact third-party's information systems that collect banking related information, for example, password managers, browsers, and search engines.

Two solutions to the problem are evident. Either expand the definition of a computer-security incident so as to include hacks/catastrophic events that impact third parties with information systems likely to have stored information or include third-parties in the definition of a bank services provider explicitly.

III. My second concern with respect to the proposed rule is that, while it may bring security and stability issues to the attention of the appropriate agencies, it does not tackle the egregious need for solutions at the regulatory level to the recent uptick in hacking. Security breaches are a serious and often unaddressed problem across the banking industry. As such, I recommend that the proposed rule, if passed, be followed by substantial review of the causes of incidents subsequently reported, as well as development of a plan of action to reduce incidents through regulation/industry cooperation.

IV. In conclusion, I wholeheartedly support the proposed rule. However, I hope that in response to the two concerns I have raised, the rule is modified so as to (1) address third party hacks, and (2) is followed by regulatory action utilizing the information provided by the notifications stemming from the rule.

Thank you in advance for your consideration of this comment.

Respectfully submitted,

Atticus Yondorf